CLAIMS

1 - Securing process for an electronic system using a cryptographic calculation procedure that uses a secret key characterised in that it consists of masking intermediate results in input or output of at least one critical function of the said procedure so that the critical function respectively gives in output or receives in input non-masked intermediate results.

2 - Process according to claim 1, characterised in that it comprises a replacement function for a critical function of the said procedure making the same calculation but with results masked in input or output.

3 - Process according to claims 1 or 2, characterised in that it consists of sequencing replacement functions so as to give non-masked results for input and output of the said procedure.

4 - Process according to one of the claims 1, 2 or 3, characterised in that it consists of using different masks according to the critical functions concerned.

5 - Process according to claim 2, characterised in that the replacement function on results masked for input is built based on the following operations:

- an operation of masking that is not public;
- an operation making the same calculation as the critical function but with results masked using the masking function.

6 - Process according to claim 2, characterised in that the

replacement function on data masked in output is built based on the following operations:

- an operation making the same calculation as the critical function but on results that must be masked by the masking function.
- A non-public masking function.

7 - Process according to one of the claims 5 or 6, characterised in that it consists of sequencing the operations of the masking function in a random manner.

8 - Electronic system comprising means to store a cryptographic calculation procedure that uses a secret key, means to carry out the said calculation procedure characterised in that it comprises means of masking intermediate results in input or output of at least a critical function of the said procedure so that the critical function respectively gives in output or receives in input non-masked intermediate results..

9 - Electronic system according to claim 8, characterised in that the masking means for intermediate results and calculation according to the critical function but with the said results masked are made of an S-box.

10 - Computer program including program code instructions to execute the steps of the process according to one of claims 1 to 7 when said program is run in an electronic system.